(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 June 2005 (23.06.2005)

PCT

(10) International Publication Number
WO 2005/057384 A1

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number:
PCT/IB2004/052728

(22) International Filing Date: 9 December 2004 (09.12.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2003/9544 9 December 2003 (09.12.2003) ZA

(71) Applicant *(for all designated States except US)*: **SMART WALLET (PTY) LIMITED** [ZA/ZA]; 371 Vine Street, Ferndale, 2194 Randburg (ZA).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **WEBBER, Glenn Andrew** [ZA/ZA]; 15 Tourmalyn Avenue, Wilro Park, 1724 Roodepoort (ZA).

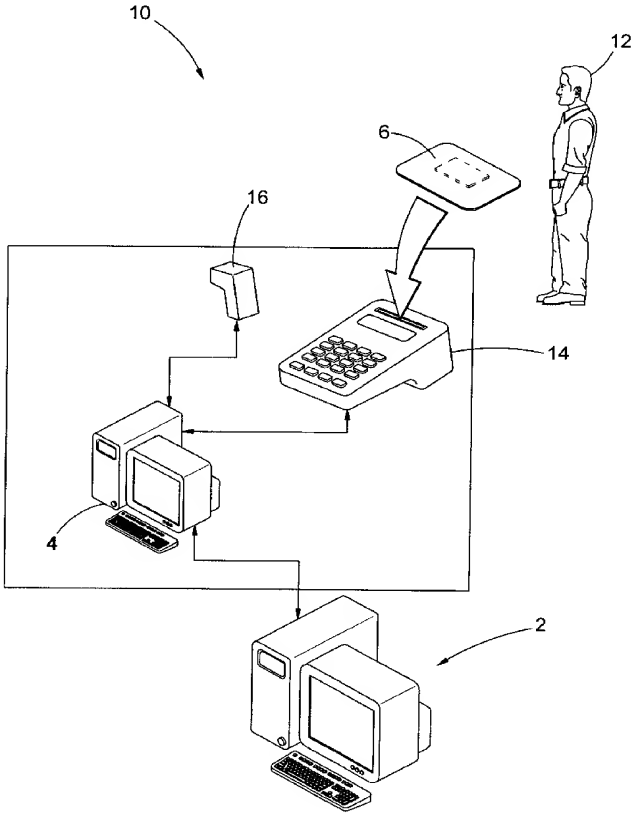
(74) Agent: **LE ROUX, Marius**; D M Kisch INC, P O Box 781218, 2146 SANDTON (ZA).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO,

[Continued on next page]

(54) Title: AN IDENTIFICATION AND AUTHORIZATION SYSTEM AND METHOD



(57) Abstract: The identification and authorization system utilises user information (including biometric user information) which is input into the system at registration to create an encrypted card key, which is stored on a smart card together with the user information and the cards unique identification number, and an encrypted storage key, which is stored on a database together with the user information and the cards unique identification number. When a transaction is requested by the user, the user information, unique identification number and encrypted card key is retrieved from the card. The user information is used to make up another encrypted card key and this is compared with the stored card key. The card key and unique identification number is then transmitted to a remote server where the encrypted card key is verified against an encrypted storage key which corresponds to the same unique identification number, and the transaction is authorised or refused based on the verification results. The system may also be used to verify the identity of the user without the requirement of sending the encrypted card key and unique identification number to a remote terminal for verification.

WO 2005/057384 A1

SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

AN IDENTIFICATION AND AUTHORIZATION SYSTEM AND METHOD

TECHNICAL FIELD

This invention relates to an identification and authorization system and method and more particularly, but not exclusively, to an electronic identification and security system for smart card.

INTRODUCTION AND BACKGROUND TO THE INVENTION

Identity fraud is a problem in society. This may involve the perpetrator assuming the identity of another person to either fraudulently steal from another, or to receive another form of benefit which is not due to the perpetrator.

The current identification system used by the government of the Republic of South Africa involves receiving information on each person applying for an identification document, and then issuing a document that is relatively difficult to forge. Although fingerprints are taken of applicants, and photographs are required, these biometric values are not actively used in assessing the identity of the person at each subsequent private and public transaction. Reliance is placed instead on the production of the initial identification (ID) document. A disadvantage of this is that the document may be obtained fraudulently or forged at a later stage, after which it may be used in any number of activities, as the

system does not prevent tampering with the document, and does not ensure that one person correlates to a single identity.

A further disadvantage is that anyone looking similar to the photograph in an ID document may produce the document as proof of identity, without there being any means of verification of the person's identification.

Additionally, a disadvantage with this system is that when an identification document is lost or stolen, it is onerous to replace the document, as the complicated ID document must be replicated. A waiting period is usually necessary, during which time the relevant person does not have any proof of identity. The cost of replacement of the document is also usually substantial.

Security systems, which verify a person's identification by means of biometric information, are available in the industry. These usually involve the user inputting biometric information (usually by means of a fingerprint or retinal scan) into a reader, after which the biometric information is sent to a server which verifies the biometric information which has been previously inputted by that person. Any information which is then subsequently required for that person is uploaded from that server, or else the verifying server gives authorisation for information to be uploaded from another server.

Smart cards are known in industry for a variety of functions, including banking security functions. They can contain a limited amount of information about a user, as they do not have much storage space. These usually operate by means of a secret Personal Identification Number (PIN) code that is stored on the card and is verified against a PIN which is input by the user. If the input PIN and the stored PIN are identical, further transactions are authorised. A disadvantage of the system is that PIN number may be stolen if it is written down by the user, and may be seen when it is keyed into any teller type machine before a transaction is carried out. Further, the PIN number may be "hacked" by virus-type computer programs which record keystrokes and send this information back to third parties.

Another disadvantage is that the information on the card itself may be tampered with. Additionally, the system is normally based on the initial production of an identity document when an account is opened in the first place.

Each transaction type (i.e. banking type transactions or retail type transactions) usually requires a separate smart card, as each card issuer is reluctant to rely on the security pre-checks and systems of another card issuer, and prefer to carry these out for themselves. This is as a result of the flaws in security mentioned above. This results in each person having to carry around a wide variety of cards, as well as an identification document. There is a risk of any of these getting lost or stolen, after which it is necessary to go though that card issuer's

security clearance procedures again (which usually involves requiring the user to produce his identification document again)

Currently, smart cards used in known systems usually carry applications on them. These applications relatively use a lot of the storage capacity of the smart card, and it is the applications that are generally "hacked" to obtain access to the information stored on the card.

Smart cards are capable of being used in several modes, notably:

- Run mode
- Download mode; and
- Test mode

To prevent hacking, the smart cards are usually issued in "Run mode". Once in this mode, the applications cannot be changed and the card cannot be used for other purposes. A disadvantage of this system is that when the application stored on the card is updated or changed, this means that all issued cards have to be replaced.

OBJECT OF THE INVENTION

It is an object of this invention to provide an identification and authorization system and method that, at least partially, alleviates some of the abovementioned disadvantages.

DISCLOSURE OF THE INVENTION

In accordance with a first aspect of this invention, there is provided an identification and authorization method comprising the steps of

receiving user information from a remote terminal, the user information including biometric information related to that user;

storing the user information on a storage means;

creating an encrypted storage key from the user information

receiving an encrypted card key that was created from user information, including biometric information, that was read off a portable storage means at a remote terminal;

comparing the encrypted card key with an encrypted storage key that was created from user information corresponding to the same user; and

transmitting the result of the comparison.

The method may further include the steps of

receiving a unique identification number that was read off a portable storage means at a remote terminal together with the user information;

storing the unique identification number together with the user information;

receiving a unique identification number that was read off a portable storage means at a remote terminal together with the encrypted card key; and

comparing an encrypted storage key, created from the stored user information corresponding to the unique identification number received with the encrypted card key, with the encrypted card key.

The method may further include the step of storing the encrypted storage key together with a reference to the unique identification number on the storage means.

The method may further include the step of comparing the biometric information relating to the user information received to biometric information already stored in the storage means.

The method may further include the steps of

assigning a unique identification number to the user information;

storing the unique identification number on a storage means with a reference to the user information; and

transmitting the unique identification number to the remote terminal for storage on the portable storage means.

The method may further include the steps of

receiving a unique identification number together with the user information, the unique identification number having being received from a portable memory means having that unique identification number;

storing the identification number together with the user information.

The identification numbers and user information may be received electronically from a network.

The network may be wireless or otherwise.

The identification numbers and user information may be received through a hard-wired network or by a radio frequency-type wireless network, or a combination of both.

The unique identification number and user information may be received from a remote terminal that is capable of reading the user information and card identification number from the card electronically.

The remote terminal may be a point-of-sale-type transaction device.

The user information and/or card identification may be stored on a storage means.

The storage means may be a computer's hard drive, and the unique identification number and user information may be stored in a database type-structure

The communication of the result may include the refusal or approval of a transaction.

The transmittal of the result of the comparison may be to the remote terminal, the user, or to a third party.

The method may further include the step of

issuing a company key to a remote terminal which, when used, will allow the remote terminal to read specific fields of encrypted information to be read off of a portable storage means.

The method may further include the step of

recording the company key and the identity of the remote terminal on a storage means.

The specific fields of information may be arranged into varying levels of confidentiality, which may be accessed by different company codes.

According to a third aspect of the invention, there is provided an identification and authorization method comprising the steps of

receiving user information, including biometric information;

creating an encrypted card key from the user information;

transmitting the user information and encrypted card key to a remote storage means;

storing the user information on a portable storage means having a unique identification number.

The method may further include the step of

encrypting the user information before storing it on the portable storage means.

The method may further include the steps of

receiving a unique identification number that has been assigned to the user information at a remote storage means; and

storing the unique identification number on the portable storage means.

The method may further include the steps of

transmitting a unique identification number corresponding to the portable storage means to the remote storage means.

The unique identification number may be assigned to the portable storage means upon storage of the user information, or it may be a permanent number.

The reception of user information and/or the unique identification number into the terminal may be accomplished by swiping a card through a card reading device, or by inputting the user information by means of keystrokes.

The terminal may a point-of-sale-type device.

The portable storage means may be a smart card.

The user information may be stored on the portable storage means in an encrypted form.

The remote storage means may be a server having a computer hard disk drive.

The user information, unique identification number and the encrypted key may be transmitted over an electronic network, or by radio frequency transmission.

According to a fourth aspect of the invention, there is provided an identification and authorization method comprising the steps of

retrieving a unique identification number and user information from a portable storage means;

creating an encrypted card key from the user information;

transmitting the unique identification number and encrypted card key to the remote storage means for the verification of the encrypted card key from the portable storage means against a previously stored encrypted storage key which was created from user information, and referenced to the same unique identification number;

receiving a communication indicating whether the verification was successful or not;

retrieving biometric information related to the user from the portable storage means;

receiving biometric user information from the user;

comparing the biometric information received from the user and the biometric information retrieved from the portable storage means in order to verify the identity of the user.

The method may further include the step of

authorising a transaction based on the verification of the identity of the user.

The portable storage means may be a smart card.

The user information retrieved from the portable storage means may be at least partially encrypted.

The remote storage means may be a server having a computer hard disk drive.

The unique identification number and/or the encrypted card key may be sent over an electronic network, or by radio frequency transmission.

The result of the comparison may be communicated by allowing or refusing a further transaction.

The method may further include the steps of

reading encrypted user information from a portable storage means; and

decrypting the user information by means of a company key received from a remote storage means.

According to a fifth aspect of the invention, there is provided an identification and authorization method comprising the step of

receiving a portable storage means having user information, a unique identification number, and an encrypted card key created from the user information stored on it.

According to a sixth aspect of the invention there is provided an identification and authorization method comprising the steps of

presenting a portable storage means, having user information, a unique identification number, and an encrypted card key created from the user information stored on it, for retrieval of the unique identification number and encrypted card key, and subsequent verification of the encrypted card key against a previously stored encrypted storage key as a means of verification of the users identity

authorising the retrieval of biometric user information from the portable storage means; and

providing biometric information for comparison against the biometric user information retrieved from the portable storage means for verification of the user's identity.

The portable storage means may further have a unique identification number stored on it that may be retrieved from the portable storage means and sent, together with the encrypted card key, for verification against an encrypted storage key associated with the same unique identification number.

According to a seventh aspect of the invention, there is provided an identification and authorization system comprising

receiving means for receiving user information from a remote terminal;

storage means for storing the user information;

instructions for encrypting the user information to create an encrypted card key from the user information;

processor means for processing the instruction; and

transmitting means for transmitting the encrypted card key to the remote terminal for storage on a portable storage means.

The system may further comprise

instructions for comparing the biometric information relating to the user information received to biometric information already stored in the storage means.

The system may further comprise

instructions for assigning a unique identification number to the user information;

instructions for storing the unique identification number on the storage means;

instructions for transmitting the unique identification number to the remote terminal for storage on the portable storage means together with the encrypted card key.

The system may further comprise

instructions for creating an encrypted storage key from the user information; and

instructions for storing the encrypted storage key on the storage means together with a reference to the unique identification number assigned to the user information.

According to an eighth aspect of the invention, there is provided an identification and authorization system comprising

receiving means for receiving an encrypted card key and a unique identification number that was read off a portable storage means at a remote terminal;

processor means for processing instructions;

instructions for retrieving an encrypted storage key that is referenced to the unique identification number from a storage means, and

instructions for comparing the encrypted storage key and the encrypted card key for the same user with each other;

storage means for storing the instructions; and

transmitting means for transmitting the result of the comparison.

The identification numbers and user information may be received electronically from a network.

The receiving and/or transmitting means may operate over a wireless network or hard-wired network, or a combination of both.

The unique identification number and user information may be received from a remote terminal that is capable of reading the user information and card identification number from the card electronically.

The remote terminal maybe a point-of-sale-type transaction device.

The storage means may be a computer's hard drive, and the unique identification number and user information may be stored in a database type-structure

The transmitting of the result may include the authorisation or rejection of a transaction.

The system may further comprise

instructions for issuing a company key to a remote terminal which will allow the remote terminal to read specific fields of encrypted information to be read off of a portable storage means.

The system may further comprise

instructions for recording the company key and the identity of the remote terminal on a storage means.

The specific fields of information may be arranged into varying levels of confidentiality, which may be accessed by different company codes.

According to a ninth aspect of the invention, there is provided an identification and authorization system comprising

receiving means for receiving user information;

biometric receiving means for receiving biometric user information;

transmitting means for transmitting user information to a remote storage means;

receiving means for receiving an encrypted card key from the remote storage means, the encrypted card key having been created from the transmitted user information; and

recording means for recording the user information and encrypted card key on a portable storage means having a unique identification number.

The system may further comprise instructions for transmitting the unique identification number of the portable storage means to the remote storage means.

The unique identification number may be assigned to the portable storage means upon storage of the user information, or it may be a permanent number.

The receiving means may include a card swiping device, or a keystroke operated input device such as a keyboard.

The system may be housed in a terminal device such as a point-of-sale-type device.

The portable storage means may be a smart card.

The user information may be stored on the portable storage means in an encrypted form.

The remote storage means may be a server having a computer hard disk drive.

The user information, unique identification number and the encrypted key may be transmitted over an electronic network, or by radio frequency transmission.

According to a tenth aspect of the invention, there is provided an identification and authorization system comprising

reading means for reading a unique identification number, and user information related to the user from a portable storage means; and

instructions for creating an encrypted card key from the user information;

transmitting means for transmitting the unique identification number and encrypted card key to the remote storage means for the verification of the encrypted card key from the portable storage means against a previously stored encrypted storage key which was created from user information, and referenced to the same unique identification number;

receiving means for receiving a communication indicating whether the verification was successful or not;

biometric receiving means for receiving biometric user information from the user;

instructions for comparing the biometric information received from the user and the biometric information retrieved from the portable storage means in order to verify the identity of the user;

storage means for storing the instructions;

processing means for processing the instructions.

The system may further comprise

instructions for authorising a transaction based on the verification of the identity of the user.

The system may be incorporated into a point-of-sale-type device.

The portable storage means may be a smart card.

The remote storage means may be a server having a computer hard disk drive.

The unique identification number and/or the encrypted card key may be sent over an electronic network, or by radio frequency transmission.

The result of the comparison may be communicated by authorising or refusing a further transaction.

The system may further comprise

instructions for reading encrypted user information from a portable storage means; and

instructions for decrypting the user information by means of a company key received from a remote storage means.

According to an eleventh aspect of the invention, there is provided an identification and authorization system comprising

a portable storage means having user information, a unique identification number, and an encrypted card key created from the user information stored on it.

The portable storage means may further have a unique identification number stored on it that may be retrieved from the portable storage means and sent, together with the encrypted card key, for verification against an encrypted storage key associated with the same unique identification number.

The portable storage means may be a smart card, or any portable electronic device having a smart card or other memory device, including a cellular telephone or Personal Digital Assistant (PDA).

According to a twelfth aspect of the invention, there is provided an identification and authorization method including the steps of

receiving user information from a user, the user information including

user information which is to remain unencrypted,

user information to be encrypted, and

biometric user information related to that user;

creating a first-type encrypted card key from the information which is to remain unencrypted, the first-type encrypted card key for use in encrypting and decrypting the user information to be stored on the portable storage means in encrypted format and biometric user information;

encrypting the user information to be stored on the portable storage means in encrypted format and the biometric information;

storing the unencrypted user information, encrypted user information, and encrypted biometric information on the portable storage means;

creating a second-type encrypted card key from the encrypted user information and the encrypted biometric information; and

storing the second-type encrypted card key on the portable storage means.

The method may include the step of

reading a unique identification number from the portable storage means;

sending the user information and unique identification number to a remote storage means.

The storage and/or encryption of the user information and biometric information on the portable storage means may be by means of stignography.

According to a thirteenth aspect of the invention there is provided an identification and authorization method including the steps of

reading stored information off a portable storage means, the information including

unencrypted user information,

encrypted user information,

encrypted biometric user information,

a second-type encrypted card key created from at least part of the encrypted user information and at least part of the biometric user information;

creating a second-type encrypted card key from at least part of the encrypted user information and at least part of the biometric user information;

verifying the stored second-type encrypted card key with the created second-type encrypted card key.

The method may further include the steps of

creating a first-type encrypted card key from the unencrypted user information;

decrypting the encrypted biometric user information using the first-type encrypted card key.

The method may further include the steps of

receiving biometric information from a user

comparing the biometric information received from the user to the unencrypted biometric information.

The method may further include the steps of

decrypting at least part of the encrypted user information using the first-type encrypted card key.

These and other features of the invention are described in more detail below.

SPECIFIC EMBODIMENT OF THE INVENTON

An embodiment of the invention is described below, purely as an example, without limiting the scope of the invention, with reference to the accompanying drawing (Figure 1) which shows a schematic representation of an identification and authorization system.

The same reference numerals are used to denote corresponding parts in the accompanying drawings.

With reference to the drawing, an identification and authorization system is generally indicated by reference numeral 10.

The identification and authorization system (10) includes a server (2), which has receiving means (not shown) such as a radio frequency (RF) receiver or network card and network connection point to a network, for receiving user information from a remote terminal such as a point-of-sale-type device (4) or a personal computer (PC) terminal, the server (2) further having storage means such as a computer hard disc (not shown) or other digital memory for storing the user information (in a database-type arrangement) and for storing instructions (not shown) for manipulating information, and transmitting means (not shown) such as a network card or network connection point for transmitting manipulated information.

The server (2) is connected through a network (8) to a remote terminal (4). The remote terminal has a card reading device (14) such as a point-of sale-type device or a card-reading device attached to a PC terminal that is capable of reading information from a portable storage means such as a smart card (6), as well as a biometric information reading device (16), such as a retinal scanner or a fingerprint reader with which to receive biometric information from a user (12). It is envisaged that a single point-of-sale type device could be the remote terminal, and could include the card reading device (14) and biometric information reading device (16). The portable storage means could also be any convenient portable memory means such as the memory on a cellular phone, a personal digital assistant or a memory stick device.

The remote terminal (4) may also have some form of card writing device (not shown) with which to write to the smart card, however this is not essential, except in the case of initial user (12) registration or when information on the card is updated.

It is envisaged that the owner and operator of a remote terminal (4) will be a service provider such as a government department, a retailer, a bank, or any business that requires positive proof of identification in order to authorise a transaction, such as airline services etc.

The initial user registration will be carried out on remote terminal having appropriate input means such as a scanner, keyboard, and the like. A user (12) will initially register him- or her-self on the system by approaching a service provider having access to a remote terminal (4) that has appropriate levels of authorisation from the central server (2) to edit user information stored on the server (2), and the user's user information will be input into a remote terminal (4). The user information inputted must include some form of biometric information that is unique to that user (12), such as a retinal scan or a fingerprint.

The user information, including the biometric information, will then be transmitted to the central server (2) where it will be received and stored (most probably in a database). Before storage of the information in the database, the biometric information will be checked against other user's biometric information stored on the server database. Should the biometric information correspond to other biometric information belonging to a prior registered user, then registration will be refused. In this way one person cannot be registered as multiple personas on the database.

If no prior registered user information corresponds to the biometric user information, card key encryption instructions (not shown) will then create an encrypted card key from the user information received, and a unique identification number (not shown) will be assigned to that encrypted card key. The unique identification number will then be stored in the server's database

together with the user information. It is envisaged that the encrypted card key will be stored as an encrypted storage key together with the user information; although alternatively the encrypted storage key may be recreated from the user information the next time it is required.

The encrypted card key and unique identification number will then also be transmitted to the remote terminal (4) for storage on the smart card (6), together with the user information as input by the user. The user information is heavily encrypted before being stored on the smart card (6).

It is envisaged that this initial registration service provider would be a governmental department, the providers of the identification and authorization system (10), or a registration service provider for a retailer. It is envisaged that the central server (2) could be connected to a central government identification database (not shown) to provide up to date identification data to the government.

When the user (12) next approaches a service provider having a remote terminal (4) for a transaction where the user's identification is required to be verified, the user (12) will insert his smart card (6) into the card reading device (14) where the unique identification number will be read off the smart card (6). Software (not shown) on the remote terminal will then create an encrypted card key from the user information stored on the smart card (6) by the same method used to create the encrypted storage key. Although the software has access to the encrypted

information on the card (6), the service provider will not have access to the information. The encrypted card key and the unique identification number are then sent to the server (2) where the corresponding unique identification number is found. The encrypted storage key corresponding to that unique identification number is then retrieved from the database, either by retrieving the stored encrypted storage key, or by making up the encrypted storage key from the stored user information corresponding to that unique identification number.

The encrypted storage key and the encrypted card key are then verified against each other. Should the encrypted card key and the encrypted storage key not match, this will indicate that either the information on the card or the information at the central server has been tampered with. A communication of the verification of the encrypted card key and the encrypted storage key is then sent to the remote terminal. This communication may be in the form of an authorisation or non-authorisation of a transaction.

If the encrypted card key and encrypted storage key do not match, the service provider at the remote terminal will be entitled to refuse to carry out any subsequent transaction.

If the encrypted card key and encrypted storage key do match then the user at the terminal will be required to input certain biometric information at the terminal. It is envisaged that the biometric information can be input while the verification is

in progress to facilitate the time required for the transaction. The corresponding stored biometric information is read off the card (6), and the two sets of biometric information are compared. If the two sets of biometric information do not match, then the service provider will be entitled to refuse the transaction. If the two sets of biometric information do match, then the service provider will authorise the transaction.

In this way the user information on the card is checked for tampering against the central server, and the identity of the user is checked against the information on the card. An advantage of this system is that for the verification process, only the unique identification number and the encrypted card key need be transmitted to the server (2), while only the result of comparison between the encrypted card key and the encrypted storage key need be transmitted to the remote terminal.

As relatively small amounts of information need to be transmitted, the bandwidth usage over the network (8) is low, which means that the time taken for verification of a user's identity will be shorter than if all of the actual information had to be transmitted across the network. It is envisaged that this system is ideally suited for communications protocols that transmit discrete packages of information, such as the General Packet Radio Service (GPRS) protocol.

Certain service providers will only have authorisation to read specific information from the card. This is accomplished by the issuing of a company key to service

providers, which only allows access to specific information fields, depending on the nature of the service provider, and the nature of the transaction. Some transactions may require only verification of the user's name, while others may require marital status, birth date, identification number, etc.

In this manner it is envisaged that the identification and authorization method and system (10) embodied will provide a secure, traceable method of providing identification and authorisation that can be utilised for a multitude of industries and functions, including many governmental functions, such as licensing of vehicle drivers, issuing of passports, recordal of person's status, issuing of pensions, and a number of others, and will provide security against the registration of one person under a number of personas.

A further benefit of this system is that new identification smart cards (6) may be issued with relative ease if they get lost, merely by downloading the information onto a smart card (6) at a remote terminal (4) after receiving biometric information from the user (12) and sending it to the server for matching with currently stored biometric information.

To avoid excessive use of bandwidth by the transmitting and receiving of user information, encryption card keys and verification results, it is envisaged that the system (10) can be used successfully to verify the identification of the user (12) and check for tampering of the smart card (6) without sending the encrypted card

key and unique identification number to the central server (2) at every transaction.

This method includes the step of receiving user information from a user (12). The user information includes three specific types of user information. The first type is user information that is to remain unencrypted, which would normally include the user's name and identity (ID) number, or other non-confidential-type information. This user information typically is information that the user (12) would have no objections to being available to every person that he expects to transact with. The second type of user information is user information that is to be encrypted on the smart card, which can include the users drivers licence, passport, bank card details, retail account details, any club memberships, medical aid details, blood group, or any other information which may be required for a transaction. This type of information is of a more confidential nature, which the user (12) would normally not want to be available to every person that he is transacting with, for personal, security or for whatever reason. The third type of user information is biometric user information related to that user, such as fingerprint details, retinal scans, a picture, or any other such information.

A first-type encrypted card key is then created from the first type of user information, that is, information that is to remain unencrypted. The first-type encrypted card key is for use in encrypting and decrypting the second type of user information, that is, user information which the user would not ordinarily

want to be available to the other party at every transaction, as well as the biometric information. The second type of user information and the biometric information is then encrypted and stored in encrypted format on a portable storage means such as a smart card (6), the memory of a personal digital assistant, the memory of a cellphone, and the like. The encryption and storage process can be by means of stignography, wherein the information is encrypted and stored within a digital image. The unencrypted (first type) user information is then also stored on the smart card (6) in unencrypted form.

A second-type encrypted card key is created partly from the encrypted user information (the second type of user information) and partly from the encrypted biometric information. This second-type encrypted card key is then also stored on the smart card (6). The smart card (6) will then be issued to the user (12).

All of the user information, together with a unique identification number associated with that smart card (6) is then sent to a remote storage means such as a database server (2) for storage.

Whenever any of the user information is updated or changed, the same procedure is followed as above, and the updated information will be sent to the remote database server (2).

The advantage of this is that if the smart card (6) is lost or damaged, a new card may be issued easily and quickly, with the user information being available online from the database server (2).

When the user (12) wants to undertake any transaction in which his identity is to be verified, he will produce the smart card (6), and it will be inserted into a card-reading device (14), such as a point-of-sale device connected to a remote PC terminal (4).

The information previously stored on the smart card (6) will be read off, the information including the unencrypted user information (the first-type user information), the encrypted second-type user information, the encrypted biometric user information, and the second-type encrypted card key.

Another second-type encrypted card key will then be created partly from the encrypted user information (the second type of user information) and partly from the biometric information, using the same algorithm that was used to create the stored second-type encrypted card key.

The stored second-type encrypted card key and the newly created second-type encrypted card key will then be compared to verify that there has been no tampering with either the encrypted biometric information or the encrypted (second type) user information.

Once the encrypted biometric and encrypted (second type) user information has been checked for tampering, the unencrypted (first type) user information will be read off the smart card (6), and used to create a first-type encrypted card key, which is then used to decrypt the encrypted (second type) user information and the encrypted biometric information. If the unencrypted (first type) user information has been tampered with, then the decrypted (second type) user information will not make sense, and the decrypted biometric information will be incorrect.

The user (12) will then input his biometric information by means of a biometric scanner (16) such as a fingerprint reader, retinal scanner, or photograph. This biometric information is then compared to the decrypted biometric information from the smart card (6) to verify the user's identity.

In this manner, information is only transmitted to the remote database server (2) when any of the user information is to be updated, and bandwidth usage is avoided. Further, the card can be used "offline" to verify the user's identity.

It is envisaged that an important feature of the system will be the fact that only heavily encrypted user information will be stored on the smart card or other portable storage means, together with a small security application which encrypts, processes and stores the information. It is anticipated that data will be

encrypted using "Blowfish" technology. The information stored, as well as the application together are not expected to require much storage capacity. An advantage of this feature is that it will ensure that the card can be used for a wide variety of purposes before the storage capacity of the card is full. An added advantage of this system is that, because there is only one application on the card, which heavily encrypts the stored information, the information will be less likely to be "hacked".

Further, a wide variety of biometric information, corresponding to various biometric parameters as well as different biometric measurement protocols and algorithms used by different scanning systems, may be stored on the card.

As the identification and authorization method and system described above acts as a means to verify the identity of the user, it is envisaged that the identification and authorization method and system described above can be applied to various fields of application. For example, the system may be used to ensure secure Internet access for Internet and e-commerce based transactions. The system further can be applied to ensure secure email communications and file encryption, by acting as a form of private-private key encryption, which is based on biometric information. Additionally, the system may be used in a document archiving system, creating a virtual safe from which files may only be opened by the person to whom the files are addressed. Other envisaged field of application are that of physical access control, and PC security.

The identification and authorization method and system further finds application on portable electronic devices such as cellular telephones, personal digital assistants, laptop computers and the like, as part of the verification of the owner when the device is switched on. This field of application will become more viable as more portable electronic devices are produced which may read biometric information, or as biometric information readers are sold as accessories for such devices. In this situation, the users own cellular telephone or other portable electronic device will function as the remote PC terminal, and the memory of the portable electronic device will function as the portable storage means. This system would ensure that the portable electronic device could not be accessed by anyone other than the user if the phone is lost or stolen, even if it is still active.

It is further envisaged that the identification and authorization method and system can be utilised as a security layer, which may be overlaid on known credit card systems, such as the Electron-MasterCard-Visa (EMV) system, as the system does not utilise large amounts of memory.

A further important aspect of the identification and authorization method and system is that it allows current smart cards to be used in "Test mode", where other current systems are only used in "Run mode" to prevent hacking of the various application held on the card. If and when the application on the card is

updated, all of the issued cards may merely be taken in for updating, and will not have to be replaced.

It will be appreciated that numerous embodiments of the invention may be performed without departing from the scope of the invention as disclosed above.

CLAIMS

1. An identification and authorization method comprising the steps of

receiving user information from a remote terminal, the user information including biometric information related to a corresponding user;

storing the user information on a storage means;

creating an encrypted storage key from the user information;

receiving an encrypted card key that was created from user information, including biometric information, that was read off a portable storage means at a remote terminal;

comparing the encrypted card key with an encrypted storage key that was created from user information corresponding to the same user; and

transmitting the result of the comparison.

2. The method as claimed in claim 1 further including the steps of

receiving a unique identification number that was read off a portable storage means at a remote terminal together with the user information;

storing the unique identification number and the user information;

receiving a unique identification number that was read off a portable storage means at a remote terminal together with the encrypted card key; and

comparing an encrypted storage key, created from the stored user information corresponding to the unique identification number received with the encrypted card key, with the encrypted card key.

3. The method as claimed in claim 1 or 2, further including the step of storing the encrypted storage key together with a reference to the unique identification number on the storage means.

4. The method as claimed in claim 1, 2 or 3, further including the step of comparing the biometric information relating to the user information received to biometric information already stored in the storage means.

5. The method as claimed in any of claims 1-4, further including the steps of assigning a unique identification number to the user information;
storing the unique identification number on a storage means with a reference to the user information; and
transmitting the unique identification number to the remote terminal for storage on the portable storage means.

6. The method as claimed in any of claims 1-5, further including the steps of receiving a unique identification number together with the user information, the unique identification number having being received from a portable storage means having that unique identification number; and
storing the identification number together with the user information.

7. The method as claimed in any of claims 1-6, wherein the identification numbers and user information is received electronically through a network.

8. The method as claimed in claim 7, wherein the identification numbers and user information are received through a hard-wired network.

9. The method as claimed in claim 7, wherein the identification numbers and user information are received through a radio frequency-type wireless network.

10. The method as claimed in claim 7, wherein the identification numbers and user information are received through a combination of both a hard-wired network and a radio frequency-type wireless network.

11. The method as claimed in any of claims 1-10, wherein the unique identification number and user information are received from a remote terminal that is capable of reading the user information and card identification number from the card electronically.

12. The method as claimed in claim 11, wherein the remote terminal may be a point-of-sale-type transaction device.

13. The method as claimed in any of claims 1-12, wherein the user information and/or card identification is stored on a storage means.

14. The method as claimed in claim 13, wherein the storage means is a computer's hard drive, and the unique identification number and user information is stored in a database type-arrangement.

15. The method as claimed in any of claims 1-14, wherein the step of the transmission of the result of the comparison includes transmitting a refusal or approval of a transaction.

16. The method as claimed in claim 15 wherein the transmission of the result of the comparison is to the remote terminal, the user, or to a third party.

17. The method as claimed in any of claims 1-16, further including the step of issuing a company key to a remote terminal which, when used, will allow the remote terminal to read specific fields of encrypted information to be read off of a portable storage means.

18. The method as claimed in any of claims 1-17, further including the step of recording the company key and the identity of the remote terminal on a storage means.

19. The method as claimed in any of claims 1-18, wherein the specific fields of information have varying levels of confidentiality, which may be accessed by different company codes.

20. An identification and authorization method comprising the steps of
receiving user information, including biometric information;
creating an encrypted card key from the user information;
transmitting the user information and encrypted card key to a remote storage means;
storing the user information on a portable storage means having a unique identification number.

21. The method as claimed in claim 20, further including the step of encrypting the user information before storing it on the portable storage means.

22. The method as claimed in claim 20 or 21, further including the step of receiving a unique identification number that has been assigned to the user information at a remote storage means; and
storing the unique identification number on the portable storage means.

23. The method as claimed in claim 20, 21 or 22, further including the step of transmitting a unique identification number corresponding to the portable storage means to the remote storage means.

24. The method as claimed in any of claims 20 to 23, wherein the unique identification number may be assigned to the portable storage means upon storage of the user information, or it may be a permanent number.

25. The method as claimed in any of claims 20 to 24, wherein the reception of user information and/or the unique identification number into the terminal is accomplished by swiping a card through a card reading device.

26. The method as claimed in any of claims 20 to 24, wherein the reception of user information and/or the unique identification number into the terminal is accomplished by inputting the user information by means of keystrokes.

27. The method as claimed in any of claims 20 to 26, wherein the terminal is a point-of-sale-type device.

28. The method as claimed in any of claims 20 to 27, wherein the portable storage means is a smart card.

29. The method as claimed in any of claims 20 to 28, wherein the user information is stored on the portable storage means in an encrypted form.

30. The method as claimed in any of claims 20 to 29, wherein the remote storage means is a server.

31. The method as claimed in any of claims 20 to 30, wherein the user information, unique identification number and the encrypted key are transmitted over an electronic network, or by radio frequency transmission, or both.

32. An identification and authorization method comprising the steps of retrieving a unique identification number and user information from a portable storage means;
creating an encrypted card key from the user information;
transmitting the unique identification number and encrypted card key to the remote storage means for the verification of the encrypted card key from the portable storage means against a previously stored encrypted storage key which was created from user information, and referenced to the same unique identification number;
receiving a communication indicating whether the verification was successful or not;
retrieving biometric information related to the user from the portable storage means;
receiving biometric user information from the user; and

comparing the biometric information received from the user and the biometric information retrieved from the portable storage means in order to verify the identity of the user.

33. The method as claimed in claim 32, further including the step of authorising a transaction based on the verification of the identity of the user.

34. The method as claimed in claim 32 or 33, wherein the portable storage means is a smart card.

35. The method as claimed in claim 32, 33 or 34, wherein the user information retrieved from the portable storage means is at least partially encrypted.

36. The method as claimed in any of claims 32 to 35, wherein the remote storage means is a server.

37. The method as claimed in any of claims 32 to 36, wherein the unique identification number is sent over an electronic network, or by radio frequency transmission.

38. The method as claimed in any of claims 32 to 37, wherein the encrypted card key is sent over an electronic network, or by radio frequency transmission.

39. The method as claimed in any of claims 32 to 38, wherein the verification of the comparison is communicated by allowing or refusing a further transaction.

40. The method as claimed in any of claims 32 to 39, further including the steps of

reading encrypted user information from a portable storage means; and decrypting the user information by means of a company key received from a remote storage means.

41. An identification and authorization method comprising the step of receiving a portable storage means having user information, a unique identification number, and an encrypted card key created from the user information stored on it.

42. An identification and authorization method comprising the steps of presenting a portable storage means, having user information, a unique identification number, and an encrypted card key created from the user information stored on it, for retrieval of the unique identification number

and encrypted card key, and subsequent verification of the encrypted card key against a previously stored encrypted storage key as a means of verification of the users identity;

authorising the retrieval of biometric user information from the portable storage means; and

providing biometric information for comparison against the biometric user information retrieved from the portable storage means for verification of the user's identity.

43. The method as claimed in claim 42, wherein the portable storage means further has a unique identification number stored on it that may be retrieved from the portable storage means and sent, together with the encrypted card key, for verification against an encrypted storage key associated with the same unique identification number.

44. An identification and authorization system comprising

receiving means for receiving user information from a remote terminal;

storage means for storing the user information;

instructions for encrypting the user information to create an encrypted card key from the user information;

processor means for processing the instruction; and

transmitting means for transmitting the encrypted card key to the remote terminal for storage on a portable storage means.

45. The system as claimed in claim 44, further comprising instructions for comparing the biometric information relating to the user information received to biometric information already stored in the storage means.

46. The system as claimed in claim 44 or 45, further comprising instructions for assigning a unique identification number to the user information;
instructions for storing the unique identification number on the storage means; and
instructions for transmitting the unique identification number to the remote terminal for storage on the portable storage means together with the encrypted card key.

47. The system as claimed in claim 44, 45 or 46, further comprising instructions for creating an encrypted storage key from the user information; and
instructions for storing the encrypted storage key on the storage means together with a reference to the unique identification number assigned to the user information.

48. An identification and authorization system comprising

receiving means for receiving an encrypted card key created from user information and a unique identification number that was read off a portable storage means at a remote terminal;

processor means for processing instructions;

instructions for retrieving an encrypted storage key that is referenced to the unique identification number from a storage means,

instructions for comparing the encrypted storage key and the encrypted card key for the same user with each other;

storage means for storing the instructions; and

transmitting means for transmitting the result of the comparison.

49. The system as claimed in claim 48, wherein the receiving means operates over a wireless network or hard-wired network, or a combination of both.

50. The system as claimed in claim 48 or 49, wherein the transmitting means operates over a wireless network or hard-wired network, or a combination of both.

51. The system as claimed in any of claims 48 to 50, wherein the unique identification number and encrypted card key are received from a remote terminal that is capable of reading the user information and card identification number from the portable storage means electronically.

52. The system as claimed in any of claims 48 to 51, wherein the remote terminal is a point-of-sale-type electronic transaction device.

53. The system as claimed in any of claims 48 to 53, wherein the storage means is a computer's hard drive, and the unique identification number and user information may be stored in a database-type arrangement.

54. The system as claimed in any of claims 48 to 54, wherein the transmitting of the result may include information authorising or rejecting a transaction.

55. The system as claimed in any of claims 48 to 54, further comprising instructions for issuing a company key to a remote terminal which will allow the remote terminal to read specified fields of encrypted information to be read off of a portable storage means.

56. The system as claimed in any of claims 48 to 53, further comprising instructions for recording the company key and the identity of the remote terminal on a storage means.

57. The system as claimed in any of claims 48 to 53, wherein the specific fields of user information are arranged into varying levels of confidentiality, which may be accessed by different company codes.

58. An identification and authorization system comprising

receiving means for receiving user information;

biometric receiving means for receiving biometric user information;

transmitting means for transmitting user information to a remote storage means;

receiving means for receiving an encrypted card key from the remote storage means, the encrypted card key having been created from the transmitted user information; and

recording means for recording the user information and encrypted card key on a portable storage means having a unique identification number.

59. The system as claimed in claim 58, further comprising instructions for transmitting the unique identification number of the portable storage means to the remote storage means.

60. The system as claimed in claims 58 or 59, wherein the unique identification number is assigned to the portable storage means on storage of the user information.

61. The system as claimed in claims 58, 59 or 60, wherein the unique identification number is a number which is assigned to the portable storage means.

62. The system as claimed in any of claims 58 to 61, wherein the receiving means includes a card swiping device, or a keystroke operated input device such as a keyboard.

63. The system as claimed in any of claims 58 to 62, wherein the system is housed in a terminal device such as a point-of-sale-type device.

64. The system as claimed in any of claims 58 to 63, wherein the portable storage means is a smart card.

65. The system as claimed in any of claims 58 to 64, wherein the user information is stored on the portable storage means in an encrypted form.

66. The system as claimed in any of claims 58 to 65, wherein the remote storage means is a server.

67. The system as claimed in any of claims 58 to 66, wherein the user information, unique identification number and the encrypted key is transmitted over an electronic network, alternatively by radio frequency transmission, alternatively by both.

68. An identification and authorization system comprising

reading means for reading a unique identification number, and user information related to the user from a portable storage means;

instructions for creating an encrypted card key from the user information;

transmitting means for transmitting the unique identification number and encrypted card key to the remote storage means for the verification of the encrypted card key from the portable storage means against a previously stored encrypted storage key which was created from user information, and referenced to the same unique identification number;

receiving means for receiving a communication indicating whether the verification was successful or not;

biometric receiving means for receiving biometric user information from the user;

instructions for comparing the biometric information received from the user and the biometric information retrieved from the portable storage means in order to verify the identity of the user;

storage means for storing the instructions; and

processing means for processing the instructions.

69. The system as claimed in claim 68, further comprising instructions for authorising a transaction based on the verification of the identity of the user.

70. The system as claimed in any claim 68 or 69, wherein the system is incorporated into a point-of-sale-type device.

71. The system as claimed in any of claims 68 to 70, wherein the portable storage means is a smart card.

72. The system as claimed in any of claims 68 to 71, wherein the remote storage means is a server.

73. The system as claimed in any of claims 68 to 72, wherein the unique identification number, alternately the encrypted card key, alternately both the unique identification number and the encrypted card key are transmitted over an electronic network, or by radio frequency transmission.

74. The system as claimed in any of claims 68 to 72, wherein the unique identification number, alternately the encrypted card key, alternately both the unique identification number and the encrypted card key are sent over by radio frequency transmission.

75. The system as claimed in any of claims 68 to 72, wherein the communication is communicated by authorising or refusing a further transaction.

76. The system as claimed in any of claims 68 to 72, further comprising instructions for reading encrypted user information from a portable storage means; and
instructions for decrypting the user information by means of a company key received from a remote storage means.

77. An identification and authorization system comprising a portable storage means having user information, a unique identification number, and an encrypted card key created from the user information stored on it.

78. The system as claimed in claim 77, wherein the portable storage means further has a unique identification number stored on it that may be retrieved from the portable storage means and sent, together with the encrypted card key, for verification against an encrypted storage key associated with the same unique identification number.

79. The system as claimed in claim 77 or 78, wherein the portable storage means is a smart card, or any portable electronic device having a smart card or other memory device, including a cellular telephone or Personal Digital Assistant (PDA).

80. An identification and authorization method including the steps of

receiving user information from a user, the user information including user information which is to remain unencrypted, user information to be encrypted, and biometric user information related to that user;

creating a first-type encrypted card key from the information which is to remain unencrypted, the first-type encrypted card key for use in encrypting and decrypting the user information to be stored on the portable storage means in encrypted format and biometric user information;

encrypting the user information to be stored on the portable storage means in encrypted format and the biometric information;

storing the unencrypted user information, encrypted user information, and encrypted biometric information on the portable storage means;

creating a second-type encrypted card key from the encrypted user information and the encrypted biometric information; and

storing the second-type encrypted card key on the portable storage means.

81. The method as claimed in claim 80, including the steps of

reading a unique identification number from the portable storage means; and

sending the user information and unique identification number to a remote storage means.

82. The method as claimed in claim 80 or 81, wherein the storage and/or encryption of the user information and biometric information on the portable storage means is by means of stignography.

83. An identification and authorization method including the steps of reading stored information off a portable storage means, the information including unencrypted user information, encrypted user information, encrypted biometric user information, a second-type encrypted card key created from at least part of the encrypted user information and at least part of the biometric user information;
creating a second-type encrypted card key from at least part of the encrypted user information and at least part of the biometric user information; and
verifying the stored second-type encrypted card key with the created second-type encrypted card key.

84. The method as claimed in claim 83, further including the steps of creating a first-type encrypted card key from the unencrypted user information; and
decrypting the encrypted biometric user information using the first-type encrypted card key.

85. The method as claimed in claim 83 or 84, further including the steps of

receiving biometric information from a user; and

comparing the biometric information received from the user to the unencrypted biometric information.

86. The method as claimed in claim 83, 84, or 85, further including the steps of decrypting at least part of the encrypted user information using the first-type encrypted card key.

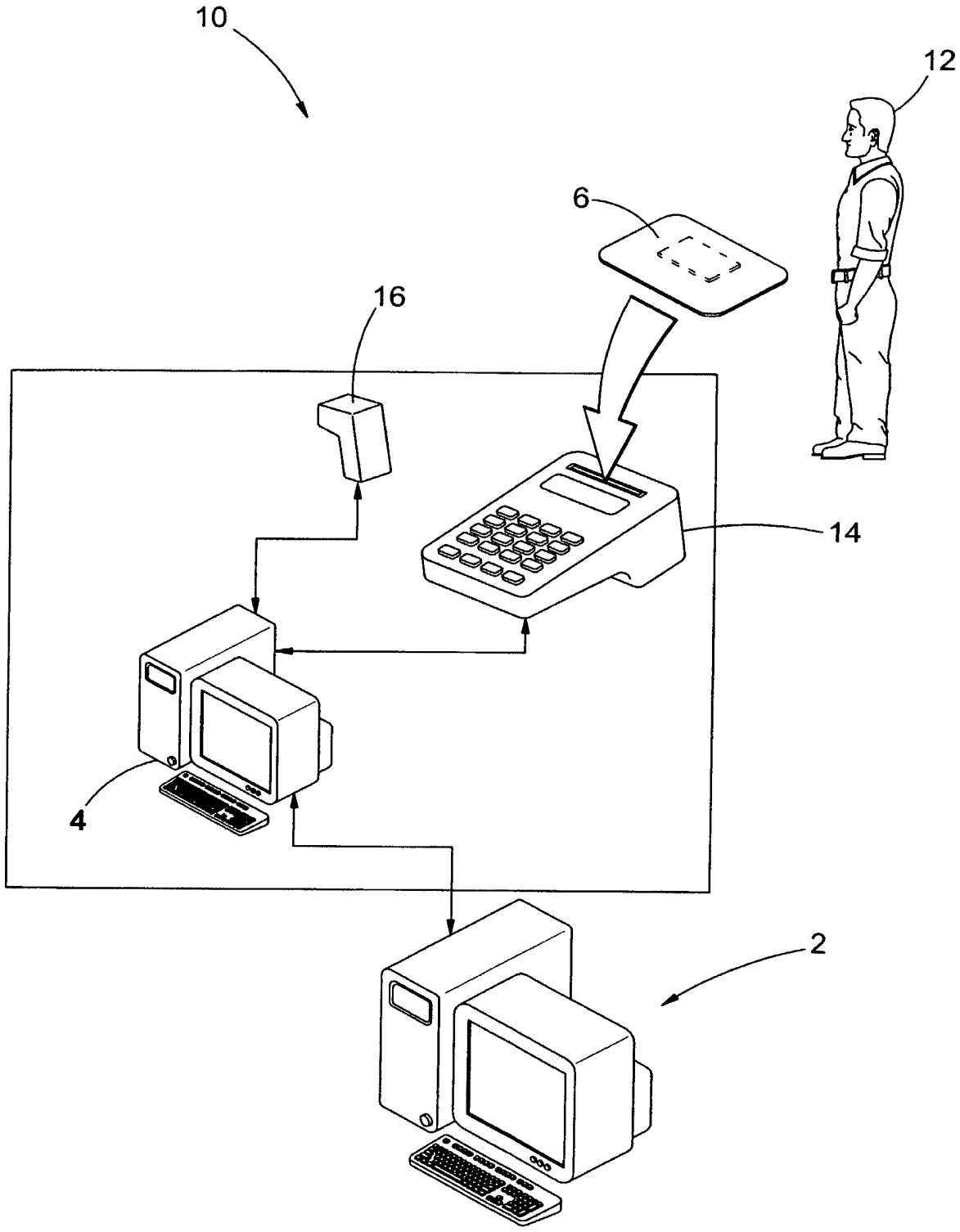


FIGURE 1

INTERNATIONAL SEARCH REPORT

IB2004/052728

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/053035 A1 (SCHUTZER DANIEL) 2 May 2002 (2002-05-02) paragraph '0010! - paragraph '0012! paragraph '0024! - paragraph '0030! -----	1-20
X	US 4 993 068 A (PIOSENKA ET AL) 12 February 1991 (1991-02-12) column 2, line 61 - column 3, line 8 column 3, line 31 - line 34 column 5, line 52 - column 6, line 48 column 7, line 7 - line 30 column 10, line 41 - column 11, line 41 ----- -/--	1-86

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 March 2005	14/03/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Alecu, M

INTERNATIONAL SEARCH REPORT

IB2004/052728

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 636 620 B1 (HOSHINO SATOSHI) 21 October 2003 (2003-10-21) column 2, line 55 - column 3, line 47 column 4, line 19 - line 29 column 5, line 63 - column 6, line 22	1,20,32, 41,42, 44,48, 58,68, 77,80,83
A	US 6 317 834 B1 (GENNARO ROSARIO ET AL) 13 November 2001 (2001-11-13) column 1, line 62 - column 2, line 25 column 4, line 57 - column 6, line 13 column 6, line 40 - column 9, line 30	1-86

INTERNATIONAL SEARCH REPORT

IB2004/052728

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002053035 A1	02-05-2002	NONE	
US 4993068 A	12-02-1991	NONE	
US 6636620 B1	21-10-2003	JP 2950307 B2	20-09-1999
		JP 11161793 A	18-06-1999
		AU 736113 B2	26-07-2001
		AU 9422298 A	17-06-1999
		CN 1221160 A ,C	30-06-1999
		GB 2331825 A ,B	02-06-1999
US 6317834 B1	13-11-2001	NONE	

PUB-NO: WO2005057384A1
DOCUMENT-IDENTIFIER: WO 2005057384 A1
TITLE: AN IDENTIFICATION AND AUTHORIZATION SYSTEM AND METHOD
PUBN-DATE: June 23, 2005

INVENTOR-INFORMATION:

NAME	COUNTRY
WEBBER, GLENN ANDREW	ZA

ASSIGNEE-INFORMATION:

NAME	COUNTRY
SMART WALLET PTY LTD	ZA
WEBBER GLENN ANDREW	ZA

APPL-NO: IB2004052728
APPL-DATE: December 9, 2004

PRIORITY-DATA: ZA200309544A (December 9, 2003)

INT-CL (IPC): G06F001/00

EUR-CL (EPC): G06F021/00 , G06F021/00

ABSTRACT:

CHG DATE=20050705 STATUS=O>The identification and authorization system utilises user information (including biometric user information)

which is input into the system at registration to create an encrypted card key, which is stored on a smart card together with the user information and the cards unique identification number, and an encrypted storage key, which is stored on a database together with the user information and the cards unique identification number. When a transaction is requested by the user, the user information, unique identification number and encrypted card key is retrieved from the card. The user information is used to make up another encrypted card key and this is compared with the stored card key. The card key and unique identification number is then transmitted to a remote server where the encrypted card key is verified against an encrypted storage key which corresponds to the same unique identification number, and the transaction is authorised or refused based on the verification results. The system may also be used to verify the identity of the user without the requirement of sending the encrypted card key and unique identification number to a remote terminal for verification.